1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2003-016286**
(43)Date of publication of application : **17.01.2003**

(51)Int.Cl. G06F 17/60
G06F 12/00
G06F 12/14

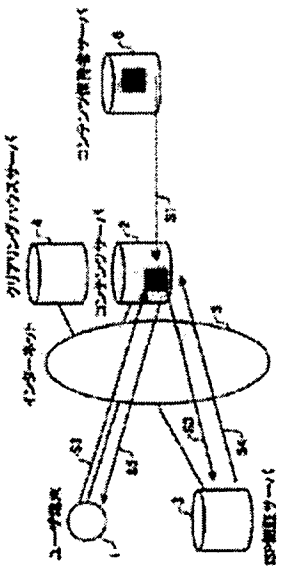
(21)Application number : **2001-199081**
(22)Date of filing : **29.06.2001**

(71)Applicant : **NTT PC COMMUNICATIONS INC**
(72)Inventor : **NAMITA HIROAKI**

(54) METHOD, SERVER AND PROGRAM FOR PROVIDING DIGITAL CONTENTS

(57)Abstract:
PROBLEM TO BE SOLVED: To provide pay digital contents to a user and to efficiently perform charging to the user.
SOLUTION: The contents server holds contents to be provided to a user terminal, the user terminal transmits user identification information and a contents request to the contents server and the contents server requests the decision of whether contents can be provided or not to the authentication server of ISP for connecting the user terminal to the Internet. Then, the authentication server decides whether the contents can be provided or not and when a notice showing that the contents can be provided is received from the authentication server, the contents server provides the contents. Then, charging is performed to the relevant user by the charging means of the ISP.

本発明のディジタルコンテンツ提供システムの基本構成を示す図



CLAIMS

[Claim(s)]

[Claim 1]It is the method of providing a user terminal with digital contents on the Internet, A content server holds contents for providing for a user terminal, A user terminal transmits user identification information and a contents request to a content server, A content server a judgment of whether to be able to provide a user terminal with demanded contents, Information about this user terminal is required of an authentication server of ISP linked to the Internet, User authentication is performed when an authentication server compares said user identification information with registration data which this authentication server holds, Judge whether this user terminal can be provided with contents, and a content server, A method that a user terminal is provided with contents when a notice of a purport that contents offer is possible is received from an authentication server, and a charging means in said ISP is characterized by performing fee collection to the contents offer concerned to the user concerned.

[Claim 2]When said content server requires a judgment of an authentication server of said ISP, This content server transmits to an authentication server with said user identification information, and information about contents an authentication server, A method according to claim 1 of judging whether said user terminal can be provided with contents based on information about these contents, and performing said fee collection based on fare information in information about these contents, while performing user authentication based on this user identification information.

[Claim 3]A method according to claim 1 of said content server accumulating a log about contents offer, and a clearing house server collecting said logs, and gathering data in this log for every holder of every ISP and contents.

[Claim 4]When permitting contents offer to the 1st user terminal, said authentication server holds information on a purport that the 1st user terminal connects, and said content server, When performing contents offer to the 1st user terminal, and information on a purport that the 1st user terminal connects is held and the 1st user terminal has received contents offer, When a contents request is made from the 2nd user terminal using the same user identification information as user identification information transmitted from the 1st user terminal, an authentication server, It is asked whether a user terminal corresponding to this user identification information connects with a content server of a connection destination of the 1st user terminal, A method according to claim 1 of continuing a judgment of contents offer propriety to the 2nd

user terminal, if a contents request from the 2nd user terminal will be refused if it is under connection, and it is not [be / it] under connection.
[Claim 5]A means to hold contents for being a content server which provides a user terminal with digital contents on the Internet, and providing for a user terminal, A means to require a judgment of whether to be able to provide a user terminal with demanded contents if user identification information and a contents request are received from a user terminal of an authentication server of ISP which connects this user terminal to the Internet, A content server having a means to provide a user terminal with contents when a notice of a purport that contents offer is possible is received from an authentication server.
[Claim 6]It is used in order to provide a user terminal with digital contents on the Internet, A means to be an authentication server in ISP which connects this user terminal to the Internet, and to receive a demand of a judgment of whether to be able to provide this user terminal with contents demanded from a user terminal from a content server, User authentication is performed by comparing user identification information received from a content server with registration data which this authentication server holds, An authentication server having a means to judge whether this user terminal can be provided with contents, and to transmit a result of a judgment to a content server.
[Claim 7]When said content server requires a judgment, this content server transmits to an authentication server with said user identification information, and information about contents this authentication server, The authentication server according to claim 6 which judges whether said user terminal can be provided with contents based on information about these contents, and performs processing for said fee collection based on fare information in information about these contents while performing user authentication based on this user identification information.
[Claim 8]When permitting contents offer to the 1st user terminal, and information on a purport that the 1st user terminal connects is held and the 1st user terminal has received contents offer, said authentication server, When a contents request is made from the 2nd user terminal using the same user identification information as user identification information transmitted from the 1st user terminal, this authentication server, Duplication of user identification information which starts a contents request based on said information is recognized, It is asked whether a user terminal corresponding to this user identification information connects with a content server of a connection destination of the 1st user terminal, The authentication server according to claim 6 which will continue a judgment of contents offer propriety to the 2nd user

terminal if a contents request from the 2nd user terminal will be refused if it is under connection, and it is not [be / it] under connection.

[Claim 9]It is a digital contents providing system which provides a user terminal with digital contents on the Internet, For every area, have two or more content servers holding contents for providing for a user terminal, and a content server of an every place region, It is connected to each ISP via a router of each ISP, is connected to an access network of an every place region via a network termination, and each content server, A means to require a judgment of whether to be able to provide a user terminal with demanded contents if user identification information and a contents request are received from a user terminal of an authentication server of ISP which connects this user terminal to the Internet, When a notice of a purport that contents offer is possible is received from an authentication server, have a means to provide a user terminal with contents, and an authentication server of each ISP, User authentication is performed by comparing user identification information received from a content server with registration data which this authentication server holds, A system having a means to judge whether this user terminal can be provided with contents, and to transmit a result of a judgment to a content server.

[Claim 10]A procedure of acquiring and holding contents for being a program which makes a computer performing processing which provides a user terminal with digital contents on the Internet, and providing for a computer at a user terminal, A procedure of requiring a judgment of whether being able to provide a user terminal with demanded contents if user identification information and a contents request are received from a user terminal of an authentication server of ISP which connects this user terminal to the Internet, A program which performs a procedure of providing a user terminal with contents when a notice of a purport that contents offer is possible is received from an authentication server.

[Claim 11]It is used in order to provide a user terminal with digital contents on the Internet, It is a program in an authentication server in ISP which connects this user terminal to the Internet, A procedure of receiving a demand of a judgment of whether being able to provide an authentication server with contents demanded from a user terminal from a content server at this user terminal, A program which performs a procedure which performs user authentication, judges whether this user terminal can be provided with contents, and transmits a result of a judgment to a content server by comparing user identification information received from a content server with registration data which this authentication server holds.

[Claim 12]When said content server requires a judgment, this content server transmits

to an authentication server with said user identification information, and information about contents said program, A procedure of judging whether said user terminal being provided with contents based on information about these contents while performing user authentication based on this user identification information, The program according to claim 11 which makes an authentication server perform a procedure of performing processing for said fee collection based on fare information in information about these contents.

[Claim 13]When permitting contents offer to the 1st user terminal and a procedure of holding information on a purport that the 1st user terminal connects, and the 1st user terminal have received contents offer, If a contents request is made from the 2nd user terminal using the same user identification information as user identification information transmitted from the 1st user terminal, Duplication of user identification information which starts a contents request based on said information is recognized, It is asked whether a user terminal corresponding to this user identification information connects with a content server of a connection destination of the 1st user terminal, The program according to claim 11 which makes an authentication server perform a procedure which will continue a judgment of contents offer propriety to the 2nd user terminal if a contents request from the 2nd user terminal will be refused if it is under connection, and it is not [be / it] under connection.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]This invention relates to the technology of charging charged digital contents by providing for a user on the Internet.

[0002]

[Description of the Prior Art]In recent years, the service which provides charged digital contents on the Internet is spreading.

[0003]In order for a contents holder to provide contents to a digital contents viewer and to perform a charge collection conventionally, For example, the hosting contractor who kept a contents holder or contents, To two or more ISP users, contents were provided, it charged with the original charge system, or one ISP kept digital contents for two or more contents holders, and the ISP had charged the user.

[0004]

[Problem to be solved by the invention]However, according to the above-mentioned

conventional technology, offer and fee collection of pay content which were uniformed were not able to be carried out easily.
[0005]This invention is 5]. This invention is made in view of the above-mentioned point, and is a thing.
The purpose provides a user with the charged digital contents which can view and listen to many and unspecified persons, Making it possible to perform fee collection to a user efficiently, a contents holder is providing the digital contents supply method and server row which make it possible to collect content rates only by depositing contents.

[0006]
[Means for solving problem]In order to attain the above-mentioned purpose, this invention can be constituted as follows.
[0007]The invention according to claim 1 is the method of providing a user terminal with digital contents on the Internet, A content server holds the contents for providing for a user terminal, A user terminal transmits user identification information and a contents request to a content server, A content server the judgment of whether to be able to provide a user terminal with the demanded contents, It requires of the authentication server of ISP which connects this user terminal to the Internet, User authentication is performed when an authentication server compares said user identification information with the registration data which this authentication server holds, It judges whether this user terminal can be provided with contents, when a content server receives the notice of the purport that contents offer is possible from an authentication server, a user terminal is provided with contents, and the charging means in said ISP performs fee collection to the contents offer concerned to the user concerned.
[0008]According to this invention, since user authentication is performed by ISP and fee collection to contents viewing is performed, it becomes possible to provide pay content efficiently. For a user, since it is not necessary to newly perform user registration etc., it becomes possible to view and listen to pay content easily.
[0009]In a description of Claim 1, when said content server requires a judgment of an authentication server of said ISP, the invention according to claim 2, This content server transmits to an authentication server with said user identification information, and information about contents an authentication server, While performing user authentication based on this user identification information, it judges whether said user terminal can be provided with contents based on information about these

contents, and said fee collection is performed based on fare information in information about these contents.
[0010]According to this invention, it becomes possible to perform access restriction according to the contents of contents.
[0011]A log concerning [on a description of Claim 1 and / said content server] contents offer in the invention according to claim 3 is accumulated, a clearing house server collects said logs and data in this log is gathered for every holder of every ISP and contents.
[0012]According to this invention, data required for billing from data in which two or more ISP and two or more contents holders were intermingled to each ISP, and charge payment to each contents holder is generable. Thereby, a contents holder becomes possible [collecting content rates only by depositing contents with a content server].
[0013]In the description of Claim 1, the invention according to claim 4 said authentication server, When permitting contents offer to the 1st user terminal, hold the information on the purport that the 1st user terminal connects, and said content server, When performing contents offer to the 1st user terminal, and the information on the purport that the 1st user terminal connects is held and the 1st user terminal has received contents offer, When a contents request is made from the 2nd user terminal using the same user identification information as the user identification information transmitted from the 1st user terminal, an authentication server, If it asks the content server of the connection destination of the 1st user terminal whether the user terminal corresponding to this user identification information connects and is connected with it, the contents request from the 2nd user terminal will be refused, and if it is not [be / it] under connection, the judgment of the contents offer propriety to the 2nd user terminal will be continued.
[0014]According to this invention, it becomes possible to prevent unlawful access by using one user ID at two or more terminals. It is possible to amend this, when the mode inconsistency of user login information arises between a content server and an authentication server.
[0015]The invention according to claim 5 is the above-mentioned content server, and the invention according to claim 6 to 8 is the above-mentioned authentication server.
[0016]The invention according to claim 9 is a digital contents providing system which provides a user terminal with digital contents on the Internet, For every area, have two or more content servers holding contents for providing for a user terminal, and a content server of an every place region, It is connected to each ISP via a router of each ISP, is connected to an access network of an every place region via a network

termination, and each content server, A means to require a judgment of whether to be able to provide a user terminal with demanded contents if user identification information and a contents request are received from a user terminal of an authentication server of ISP which connects this user terminal to the Internet, When a notice of a purport that contents offer is possible is received from an authentication server, have a means to provide a user terminal with contents, and an authentication server of each ISP, By comparing user identification information received from a content server with registration data which this authentication server holds, user authentication is performed, and it judges whether this user terminal can be provided with contents, and has a means to transmit a result of a judgment to a content server.
[0017]According to this invention, it becomes possible to provide contents so that a difference may not appear in contents quality, even if it uses which ISP.
[0018]The invention according to claim 10 to 13 is a program in each above-mentioned server.
[0019]
[Mode for carrying out the invention]Principle composition of a digital contents providing system of this invention is shown in drawing 1. First, an outline of a digital contents providing system of this invention is explained usingdrawing 1.
[0020]As shown in drawing 1, a digital contents providing system of this invention has an ISP user's user terminal 1, the content server 2, the ISP authentication server 3 of the ISP concerned, and the clearing house server 4, and takes composition in which each was connected to the Internet 5. ISP in the figure is ISP which the user concerned has joined as an Internet connectivity provider.
[0021]The contents holder server 6 shown in the figure is a server which a contents holder has, Contents holders are those to whom a person holding copyright of digital contents or copyright employment was entrusted, think that he wants many and unspecified large potential visitors to see digital contents, and deposit digital contents of self with the content server 2.
[0022]ISP is an Internet Service Provider. In this invention, when a user of the ISP concerned acquired, views and listens to contents of the content server 2, this ISP charges a content rate at the user concerned. The fee collection itself can be performed using a conventional method in a fee collection server in ISP, etc.
[0023]The user terminal 1 is a terminal of a user who wishes viewing and listening of contents, to the content server 2, establishes a connection and uses digital contents in a server.
[0024]The content server 2 is a server which a contents hosting contractor holds, and

holds a copy of a contents holder's digital contents, for example. ISP may hold the content server 2.

[0025]The clearing house server 4 is a server which a clearing house contractor holds, and performs processing for carrying out reallocation of the content rate which ISP collected to a contents holder and a contents hosting entrepreneur, for example. It is also possible to constitute the clearing house server 4 and the content server 2 from one server.

[0026]The ISP authentication server 3 holds information of a subscription user of ISP, and judges permission or denial of access to a user's contents by performing user authentication. About the ISP authentication server 3, the existing server which the ISP concerned uses for user authentication etc. can be used.

[0027]Each server is realizable by carrying a program which performs processing in this invention to a computer which has CPU, a hard disk, an input/output device, a communication control unit, etc.

[0028]An operation outline of a digital contents providing system of drawing 1is explained below.

[0029]Step 1 A contents holder deposits a copy of digital contents to the content server 2 first. It unites and fare information of the contents concerned is also notified to the content server 2. Fare information is information on ** to which it can be viewed and listened, for example, if the contents are 100 yen, or monthly amount a course of 500 yen in one viewing and listening.

[0030]Step 2 user gives the viewing-and-listening demand of pay content from the user terminal 1 to the content server 2 via the Internet 5. Then, the content server 2 requires the input of access ID or a password of a user, and a user inputs them. The access ID and password are the same as that of what is used in ISP which the user concerned has joined at the time of an Internet connectivity.

[0031]Step 3, next the content server 2 ask whether permit the user concerned viewing and listening of contents to the ISP authentication server 3. The information that it is in inquiry information (which user is what kind of fee collection about which contents) here is included.

[0032]"Which user" in the above-mentioned inquiry information is access ID and the password which the user entered, and an ISP authentication server attests whether you are a customer of the ISP concerned with this. "Which contents" are information for a user to identify the contents which required viewing and listening, and a file name, a contents holder name, a live program name, etc. are included. "What kind of fee collection" is the fare information specified when the contents holder server 6

deposited contents with the content server 2 at Step 1.
[0033]By verifying the contents of an inquiry, the ISP authentication server 3 which received step 4 inquiry information judges whether contents may be shown to a user, and returns a result of judgment to the content server 2.
[0034]Although various standards of judgment can be set up, since it is required for the user concerned to be a user of the ISP concerned in order to perform fee collection, the user concerned judges at least whether you are a your company customer from ID and a password. When viewing-and-listening refusal is carried out as other judgment, for example when applicable contents belong to a competitor, or a case where the contents of contents are not suitable for the user concerned, and a user are doing charge nonpayment to ISP, it is possible to make a judgment which carries out viewing-and-listening refusal. In order that an ISP authentication server may judge contents offer propriety, information that the contents of contents were beforehand indicated from a content server to ISP as shown in a program guide can also be transmitted. For example, control of refusing a contents request which is not in the program guide is attained.
[0035]Here, when the ISP authentication server 3 returns viewing-and-listening permission to the content server 2, if ISP charges the user concerned by accounting information contained in the contents of an inquiry and viewing-and-listening refusal is carried out, fee collection of contents will not be performed.
[0036]The step 5 content server 2 will distribute contents to the user terminal 1, if viewing-and-listening permission gets down from the ISP authentication server 3. When viewing and listening is refused, permission or denial of the access to the contents from the user terminal 1 is carried out. The content server 2 holds the result of attestation as an attestation log.
[0037] Then, the clearing house server 4 will perform processing for a charge collection. The method of a charge collection is explained using the key map shown in drawing 2.
[0038]About the contents which carried out viewing-and-listening permission, step 11ISP charges a user using a fee collection server etc. according to the appointed fare information, and collects a charge from a user. Fee collection to contents can be carried out by including in the fee collection to the usual Internet connectivity.
[0039]The step 12 clearing-house server 4 collects attestation logs from the content server 2. Thereby, the information on each ISP having carried out viewing-and-listening permission of what at which charge when at which user etc. is accumulated on the clearing house server 4.

[0040]Step 13 and a clearing house contractor charge the audience fee gold which deducted the vicarious execution collection commission according to the log accumulated on the clearing house server 4 to ISP.
[0041]Step 14ISP will pay a clearing house contractor the amount billed, if it judges that the claim of Step 13 is appropriate from the log of its company.
[0042]A clearing house contractor pays a contents hosting contractor an equipment usage fee if needed [step 15].
[0043]Step 16 A clearing house contractor pays a contents holder the audience fee of applicable contents.
[0044]A step 17 clearing-house contractor unites and submits the log of viewing and listening to a contents holder.
[0045]Next, the above-mentioned digital contents providing system is explained more to details.
[0046](System configuration) The example of the composition of the digital contents providing system of this invention is shown in drawing 3 and 4. This example is an example in the case of considering a content server as local distribution installation, shows drawing 3 an entire configuration and showsdrawing 4 the composition of each base.
[0047]As shown in drawing 3, quality of contents with which a user is provided can be uniformed by making every place distribute a content server. As shown in drawing 4, by carrying out direct continuation of the content server to each ISP in a base building, it becomes possible to provide contents, without being dependent on network composition of each ISP, and also quality can be uniformed.
[0048]Therefore, since it becomes the almost same quality even if a user uses which ISP, a contents holder can determine prices of contents.
[0049]Next, authentication technology and unlawful access permission-or-denial technology are explained as main technology in the above-mentioned digital contents providing system.
[0050](Authentication technology) The tables which the content server 2 has are shown in drawing 5. A table which the ISP authentication server 3 has is shown in drawing 6. Operation in a content server and an ISP authentication server is explained more to details using drawing 5 and drawing 6.
[0051]In drawing 5, it is a contents storage in the contents repository 7, and contents for providing for a user are stored. The contents managing table 8 has an item of a fee collection pattern for every contents, access restriction, an owner, etc. The ISP authentication server control table 9 stores a domain name and an ISP authentication

server dress corresponding to the domain name in which ISP authentication server as information for determining whether an authentication demand should be published from a domain name of user ID which carried out the connection request. It has the connected user table 10 showing a list of a user under present connection and an authentication demand, and the attestation log 11 which records event information for every notice of cutting.

[0052]As shown in drawing 6, as for a user management table which the ISP authentication server 3 holds, it has user ID, a password, access restriction, and a state.

[0053]The operation in user authentication is as follows.

[0054]First, a user who has joined ISP1 transmits an access request to the contents A by entering user ID and a password (Step 21). Then, in the content server 2, the contents managing table 8 is referred to and a fee collection pattern of the contents A, access restriction information, and an owner name of contents are extracted (Step 22).

[0055]And the content server 2 searches an address of domain name isp1 to ISP1 authentication server of ISP1 with which a user joins from the ISP authentication server control table 9, Attestation is required by transmitting information about contents, including a contents name, an owner, fare information, etc., to the addressing to an address with user ID and a password (Step 23). At this time, the contents of that authentication demand are recorded on the attestation log 11.

[0056]In ISP1 authentication server which received an authentication demand, it is attested whether the user concerned is a customer of his company, and whether it corresponds to access restriction with reference to a user management table shown in drawing 6. It is judged whether ISP1 authentication server provides contents by having contents information to which it can be viewed and listened, or viewing-and-listening prohibition contents information, and comparing contents information required as this information. Information about a charge of the contents concerned transmitted from a content server is used for contents viewing charge fee collection to the user concerned.

[0057]And the authentication result is returned to the content server 2.

[0058]When ISP1 authentication server permits contents access, an item of a "state" of a table shown in drawing 6 becomes "under connection." When the user terminal concerned connects with the content server 2 and receives offer of contents, ID of the user concerned, etc. are indicated as a user under present connection in the connected user table 10. moreover -- contents -- offer -- an end -- the time -- **** -- a connected user -- a table -- ten -- from -- being concerned -- a user -- deleting -- having -- a

content server -- contents providing service -- having completed -- a purport -- ISP -- one -- an authentication server -- notifying -- ISP -- one -- an authentication server -- being concerned -- a user -- corresponding -- user management -- a table -- " -- a state -- " -- " -- un--- connection -- " -- it carries out. These are used in unlawful access permission or denial mentioned later.

[0059](Unlawful access permission-or-denial technology) When user ID and a password perform access authentication to the content server 2 as mentioned above, others' access ID and a password are used unjustly and there is a risk of unlawful access that two or more users acquire contents simultaneously by one ID being performed. In order to prevent such unlawful access, a connected user table and a user management table which were explained in drawing 5 and drawing 6 are used. Hereafter, processing for prevention from unlawful access is explained using drawing 7 and drawing 8.

[0060]In drawing 7, a user performs an access request first to a digital content server installed in Sapporo, and it is assumed that access is permitted, and it is viewing and listening to applicable contents (Steps 31-33). At this time, an ISP authentication server makes @ Sapporo" the state corresponding to the user ID concerned in a user management table during "connection. This means that a content server of Sapporo is supplying the user concerned with service. The user ID (id1@isp1) concerned is added to a connected user table in a content server of Sapporo.

[0061]When other users perform a contents access request with same user ID and a password, for example to a content server of Tokyo while this user connected (Step 34), a user corresponding to the user ID connects an ISP authentication server which received an authentication demand by the above-mentioned user management table -- thing recognition is carried out (Steps 34 and 35).

[0062]Thus, when an ISP authentication server receives an authentication demand again to user ID under connection (double access detection), an ISP authentication server receives a content server of Sapporo, It asks whether the first user is supplying service (is the user ID concerned shown in a connected user table or not?), and if it becomes clear that the first user connects, an ISP authentication server will return a connection refusal to an authentication demand (Steps 36-38).

[0063]On the other hand, when it is checked in a content server of Sapporo that the user concerned does not connect, When authentication work is continued to an authentication demand (Step 35) of a content server of Tokyo, attestation is successful and it is judged that contents viewing is possible, contents are provided from a content server of Tokyo to the user concerned.

[0064]Drawing 8 is a flow chart which shows processing in an ISP authentication server.
[0065]If a certain access point has access from a user (Step 41), user authentication is performed (Step 42), if attestation is O.K., with reference to a user management table, it will judge whether the user concerned is [******] under connection (under login), and connection will be refused if attestation is NG. Next, with reference to a user management table, it checks whether the user concerned connects (under login) (Step 43), and connection will be permitted if it has not connected. When in under connection (under login) a state is asked to a content server under connection concerned (Step 44) and there is a reply under connection from a content server, connection is refused, and connection is permitted at the time of un-connecting (Step 45).
[0066]By checking whether it is under [connection] ****** to the content server which starts the first user access as mentioned above, By loss on reboot of a content server, and the network of an authentication packet, etc., in spite of having completed the service supply in the content server about the first user, Even when the mode inconsistency recognized that only an ISP authentication server is among service provision arises, it becomes possible to judge connection permission or denial exactly.
[0067]By conducting a double access inspection by an ISP authentication server, even when unlawful access is tried from the user belonging to a different content server, double access can be detected.
[0068](Accounting) Next, the processing which the clearing house server 4 performs is explained using drawing 9 for the charge collection explained bydrawing 2.
[0069]The clearing house server 4 collects the attestation logs shown in (a) ofdrawing 9 from each content server. The collected attestation logs have information, including viewing-and-listening time, ISP which charges a user, a user, a contents holder name, a contents name, the amount of money, etc.
[0070]Thus, it becomes possible to ask each ISP for audience fee gold by carrying out identification of multiple accounts under the same name as a single entity for every ISP, and making it the form shown in drawing 9 (b) to the log information in which two or more ISP and two or more holders were intermingled. It becomes possible to pay a contents holder the audience fee of contents by carrying out identification of multiple accounts under the same name as a single entity for every holder name, and making it the form shown indrawing 9 (c). A contents holder becomes able [which user] to grasp to which contents it viewed and listened when by providing a contents

holder with a viewing-and-listening log.
[0071]Change and application are variously possible for this invention within Claims, without being limited to the above-mentioned working example.
[0072]
[Effect of the Invention]As mentioned above, according to this invention, the contents holder can obtain a content rate, without using an original charge system by depositing contents to a contents hosting contractor.
[0073]Since the contents quality in which the end user of every ISP is almost homogeneous can be acquired by arranging two or more content servers at the place near an end user, a contents holder becomes possible [performing uniform rates], without choosing ISP.
[0074]It becomes possible to choose only the information in connection with the ISP concerned, and to collect audience fee gold to the ISP to each ISP, by processing of the clearing house server in this invention. On the other hand, to each contents holder, only the information in connection with the contents of the contents holder concerned is chosen, and it becomes possible to pay an audience fee.
[0075]It becomes possible to realize the above effective rate collection, without creating a new customer database, since it can charge by attesting using the existing attestation in ISP, a charge system, and registration data in this invention.
[0076]Therefore, when the user of ISP-A looks at the contents of ISP-B according to this invention, The fee collection of a content rate is made from ISP-A to a user, and on the other hand, when [that] the user of ISP-B views and listens to the contents of ISP-A as reverse, the fee collection of a content rate is made from ISP-B to a user. Thus, unlike the former, it becomes possible to build the relation of N:M of a contents holder and ISP.

DESCRIPTION OF DRAWINGS

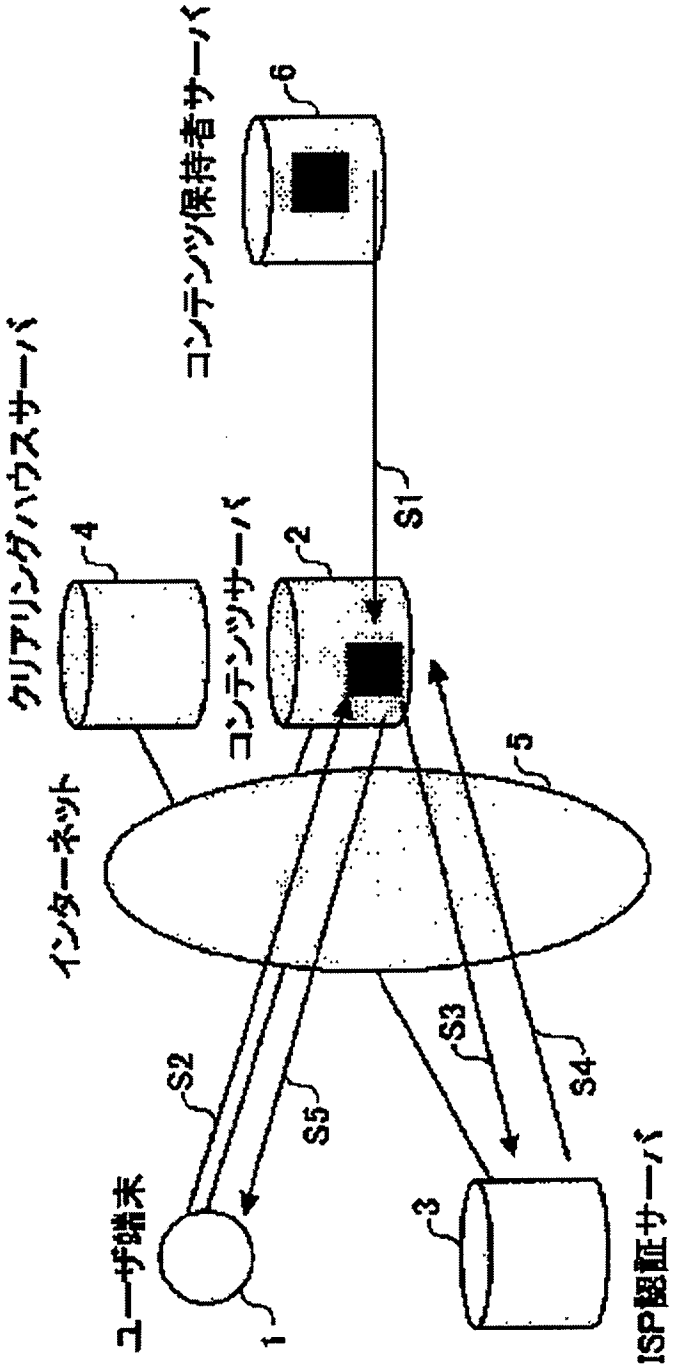
[Brief Description of the Drawings]
[Drawing 1]It is a figure showing the principle composition of the digital contents providing system of this invention.
[Drawing 2]It is a figure for explaining the method of a charge collection.
[Drawing 3]It is a figure showing the composition of a digital contents providing system.
[Drawing 4]It is a figure showing the composition of a digital contents providing

system.
[Drawing 5]It is a figure showing the tables which a content server has.
[Drawing 6]It is a figure showing the tables which an ISP authentication server has.
[Drawing 7]It is a figure for explaining unlawful access prevention technology.
[Drawing 8]It is a flow chart which shows the processing in an ISP authentication server.
[Drawing 9]It is a figure for explaining the processing in a clearing house server.
[Explanations of letters or numerals]
1 User terminal
2 Content server
3 ISP authentication server
4 Clearing house server
5 Internet
6 Contents holder server
7 Contents repository
8 Contents managing table
9 ISP authentication server control table
10 Connected user table
11 Attestation log

DRAWINGS

[Drawing 1]

本発明のディジタルコンテンツ提供システムの原理構成を示す図

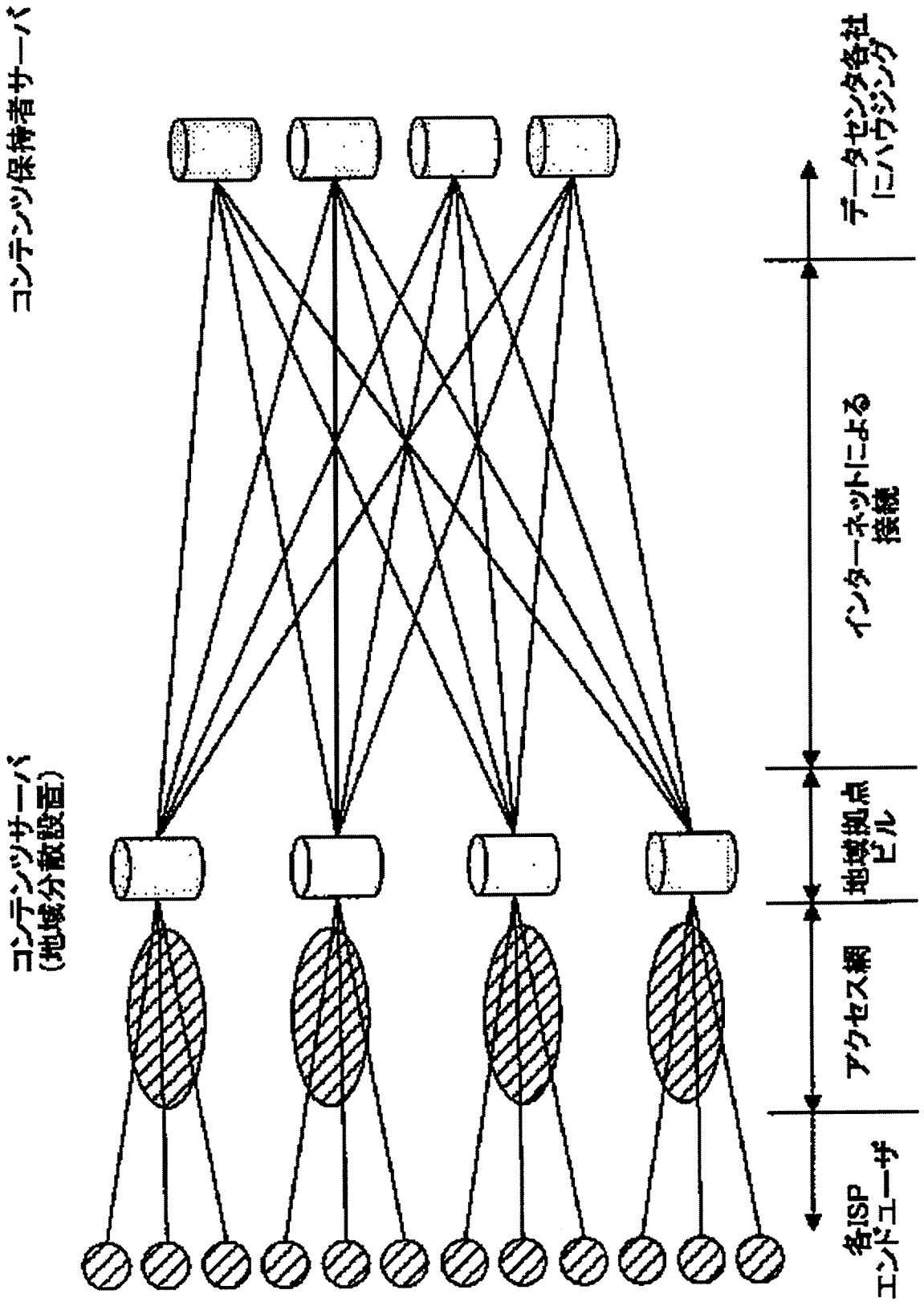


[Drawing 2]

料金回収の方法を説明するための図

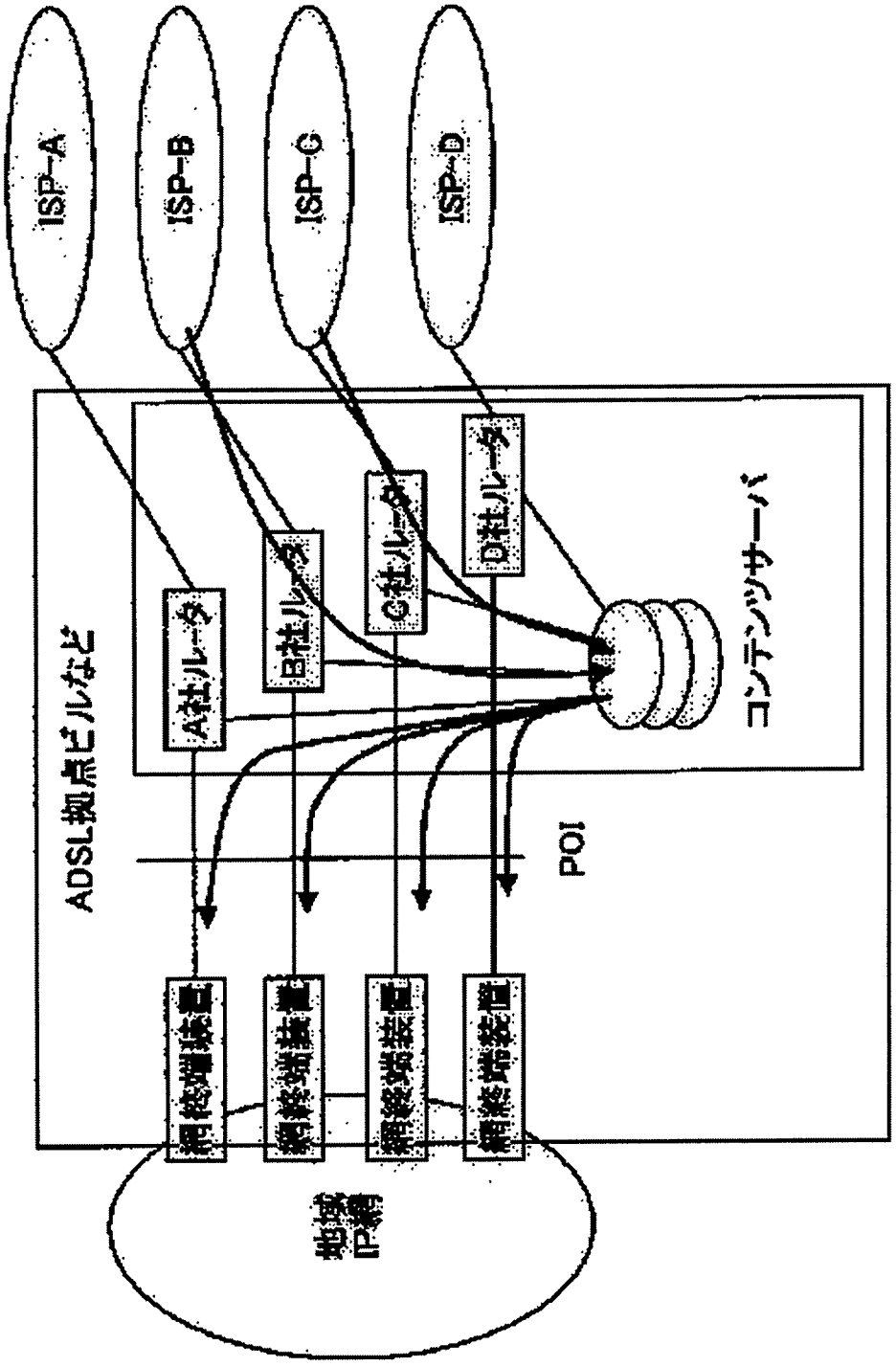
[Drawing 3]

ディジタルコンテンツ提供システムの構成を示す図

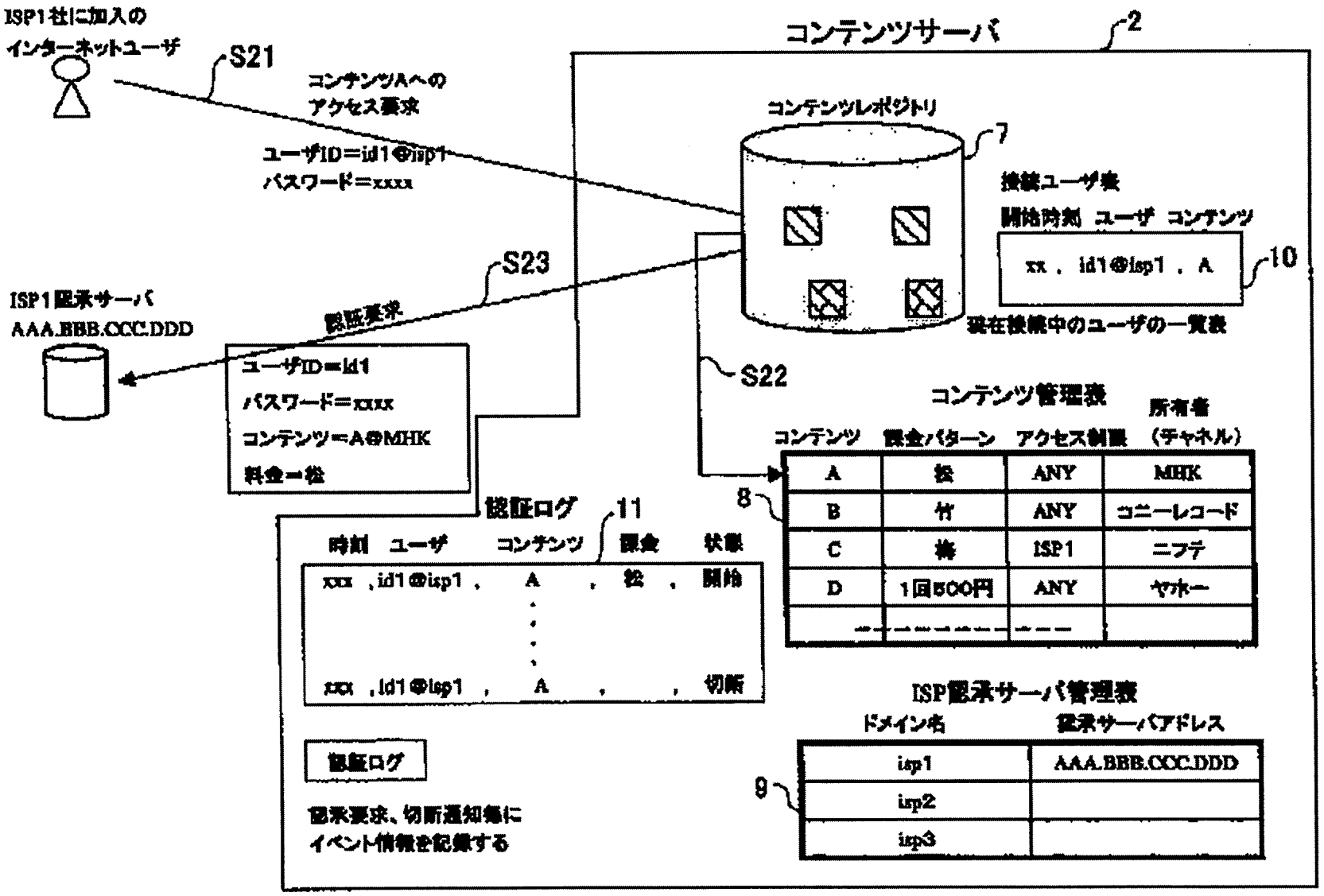


[Drawing 4]

ディジタルコンテンツ提供システムの構成を示す図



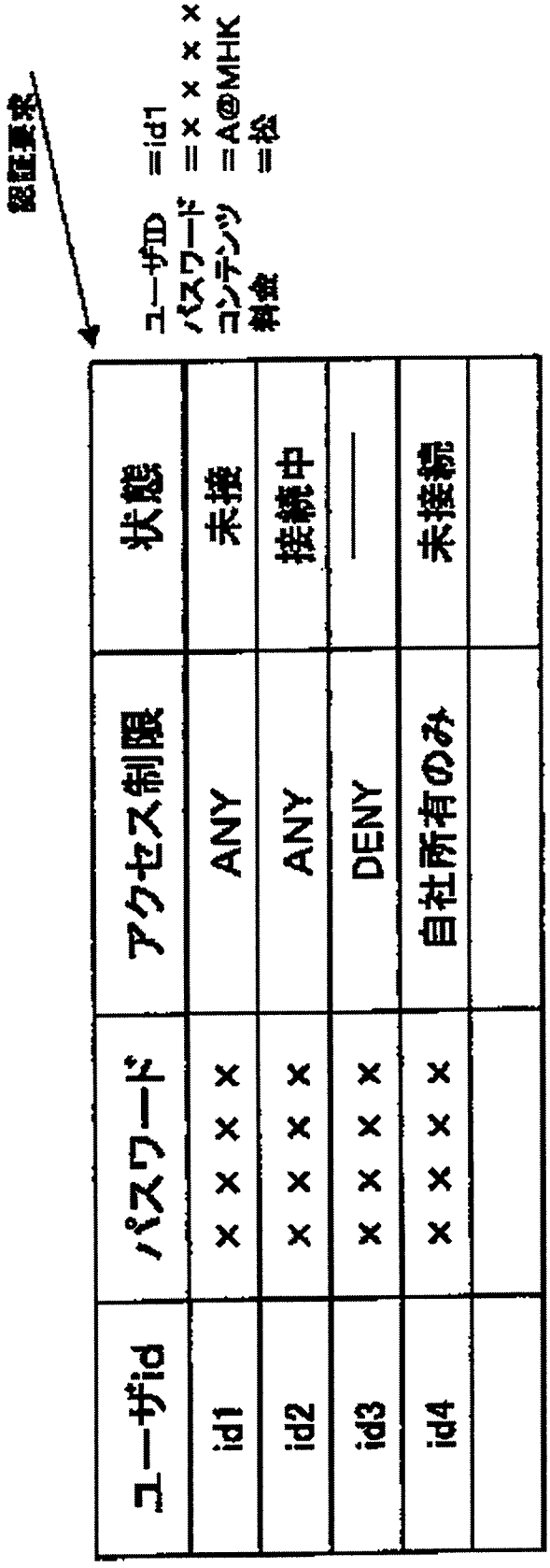
[Drawing 5]



コンテンツサーバが有するテーブル類を示す図

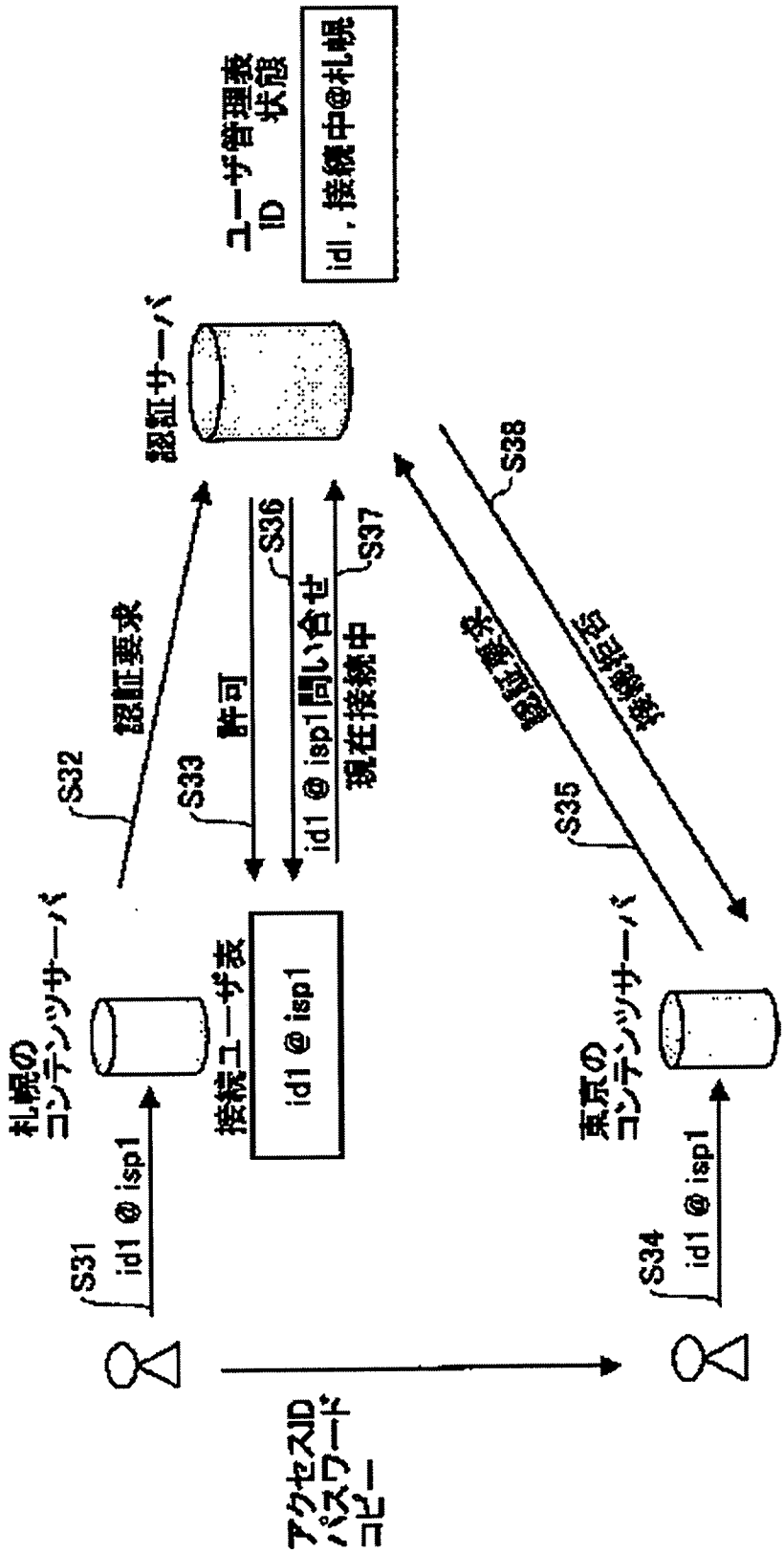
[Drawing 6]

ISP認証サーバが有するテーブル類を示す図

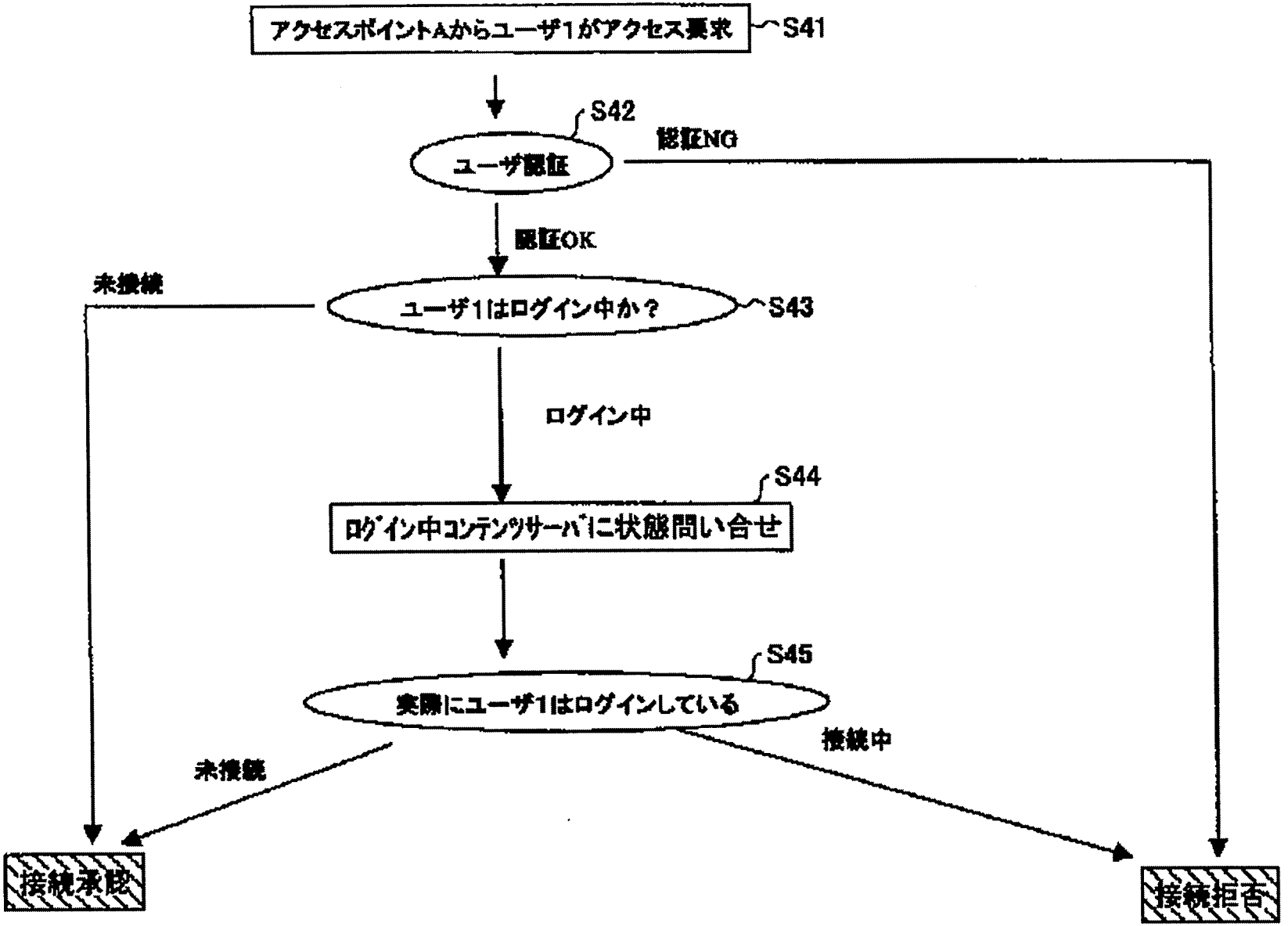


[Drawing 7]

不正アクセス防止技術を説明するための図



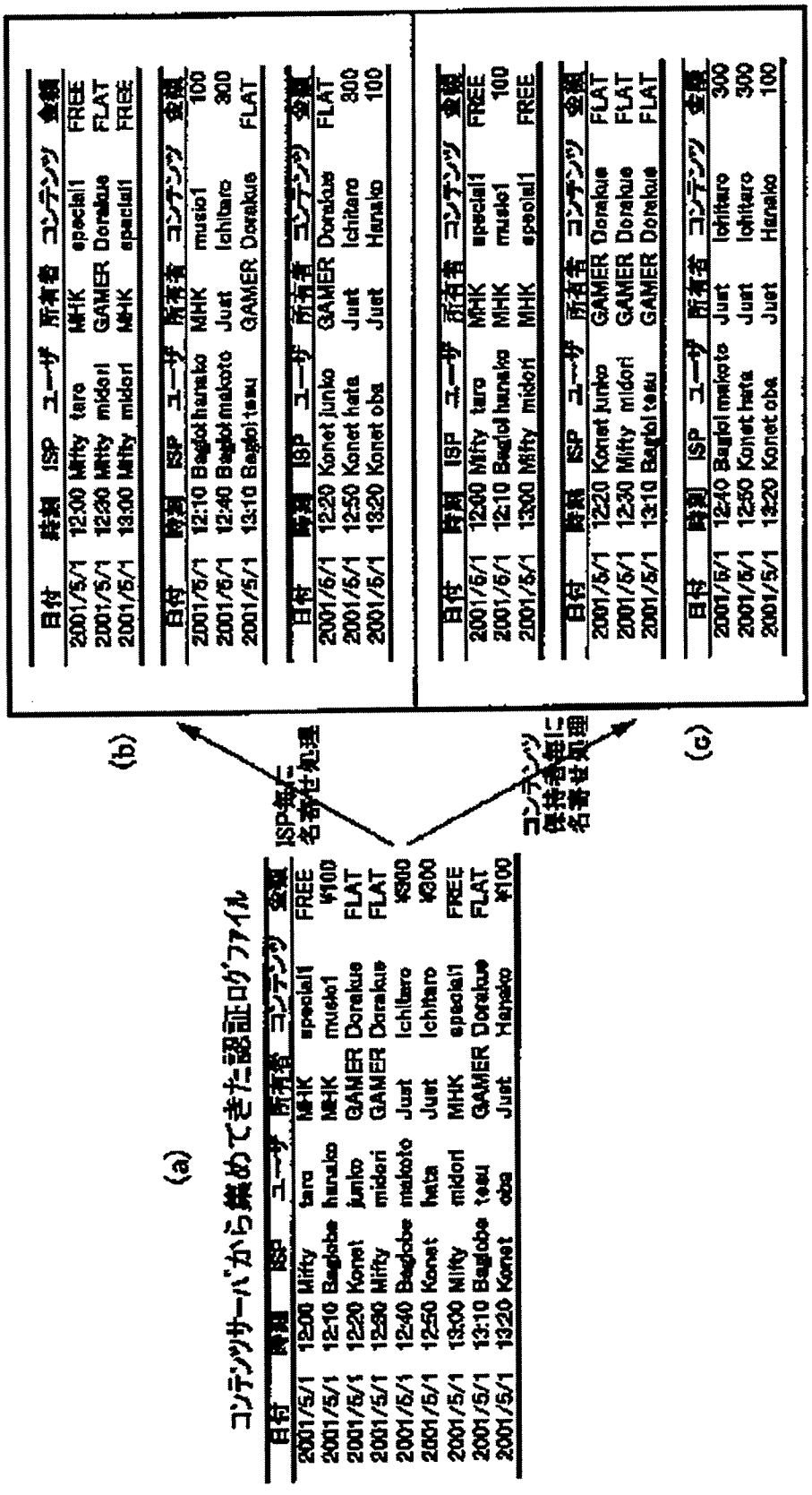
[Drawing 8]



IPS認証サーバにおける処理を示すフローチャート

[Drawing 9]

クリアリングハウスサーバにおける処理を説明するための図



PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-016286
(43)Date of publication of application : 17.01.2003

(51)Int.Cl. G06F 17/60
G06F 12/00
G06F 12/14

(21)Application number : 2001-199081
(22)Date of filing : 29.06.2001

(71)Applicant : NTT PC COMMUNICATIONS INC
(72)Inventor : NAMITA HIROAKI

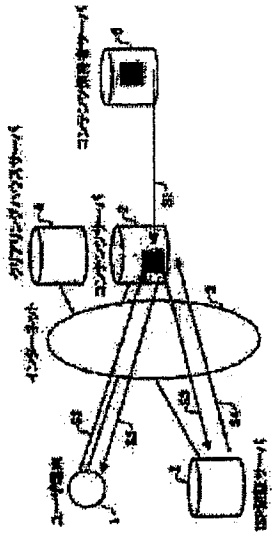
(54) METHOD, SERVER AND PROGRAM FOR PROVIDING DIGITAL CONTENTS

(57)Abstract:

PROBLEM TO BE SOLVED: To provide pay digital contents to a user and to efficiently perform charging to the user.

SOLUTION: The contents server holds contents to be provided to a user terminal, the user terminal transmits user identification information and a contents request to the contents server and the contents server requests the decision of whether contents can be provided or not to the authentication server of ISP for connecting the user terminal to the Internet. Then, the authentication server decides whether the contents can be provided or not and when a notice showing that the contents can be provided is received from the authentication server, the contents server provides the contents. Then, charging is performed to the relevant user by the charging means of the ISP.

本発明のディジタルコンテンツ提供システムの概略構成を示す図



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2003－16286
（P2003－16286A）
(43)公開日　平成15年１月17日(2003.1.17)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード(参考)
Ｇ０６Ｆ　17/60	３０２	Ｇ０６Ｆ　17/60	３０２Ｅ	５Ｂ０１７
	２２２		２２２	５Ｂ０８２
	３３０		３３０	
	３３２		３３２	
	５０２		５０２	

審査請求　有　　請求項の数13　ＯＬ　（全 12 頁）　最終頁に続く

(21)出願番号　特願2001－199081(P2001－199081)

(22)出願日　平成13年６月29日(2001.6.29)

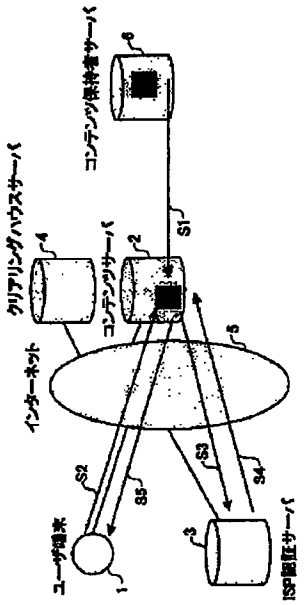
(71)出願人　397014282
株式会社エヌ・ティ・ティ　ピー・シーコミュニケーションズ
東京都港区新橋６－１－11
(72)発明者　波多　浩昭
東京都港区新橋６丁目１番11号　株式会社エヌ・ティ・ティピー・シーコミュニケーションズ内
(74)代理人　100070150
弁理士　伊東　忠彦

Ｆターム(参考)　5B017 AA03 BA05 CA16
5B082 EA12 HA05 HA08

(54)【発明の名称】　ディジタルコンテンツ提供方法及びサーバ並びにプログラム

(57)【要約】
【課題】　有料ディジタルコンテンツをユーザに提供し、効率的にユーザへの課金を行う。
【解決手段】　コンテンツサーバが、ユーザ端末に提供するためのコンテンツを保持し、ユーザ端末が、ユーザ識別情報及びコンテンツ要求をコンテンツサーバに送信し、コンテンツサーバが、コンテンツを提供できるか否かの判定を、該ユーザ端末をインターネットに接続するＩＳＰの認証サーバに要求し、認証サーバが、コンテンツを提供できるか否かの判定を行い、コンテンツサーバが、認証サーバからコンテンツ提供可能の旨の通知を受けたときにコンテンツを提供し、前記ＩＳＰにおける課金手段が当該ユーザに課金を行う。

本発明のディジタルコンテンツ提供システムの原理構成を示す図



1

【特許請求の範囲】

【請求項１】　インターネット上でディジタルコンテンツをユーザ端末に提供する方法であって、

コンテンツサーバが、ユーザ端末に提供するためのコンテンツを保持し、

ユーザ端末が、ユーザ識別情報及びコンテンツ要求をコンテンツサーバに送信し、

コンテンツサーバが、要求されたコンテンツをユーザ端末に提供できるか否かの判定を、該ユーザ端末に関する情報をインターネットに接続するＩＳＰの認証サーバに要求し、

認証サーバが、前記ユーザ識別情報と該認証サーバが保有する登録データとを比較することによりユーザ認証を行い、コンテンツを該ユーザ端末に提供できるか否かの判定を行い、

コンテンツサーバが、認証サーバからコンテンツ提供可能の旨の通知を受けたときにユーザ端末にコンテンツを提供し、

前記ＩＳＰにおける課金手段が当該ユーザに当該コンテンツ提供に対する課金を行うことを特徴とする方法。

【請求項２】　前記コンテンツサーバが前記ＩＳＰの認証サーバに判定を要求する際に、該コンテンツサーバは前記ユーザ識別情報とともにコンテンツに関する情報を認証サーバに送信し、

認証サーバは、該ユーザ識別情報に基づきユーザ認証を行うとともに、該コンテンツに関する情報に基づき前記ユーザ端末にコンテンツを提供できるか否かを判定し、該コンテンツに関する情報の中の料金情報に基づき前記課金を行う請求項１に記載の方法。

【請求項３】　前記コンテンツサーバは、コンテンツ提供に関するログを蓄積し、

クリアリングハウスサーバが、前記ログを収集し、該ログにおけるデータをＩＳＰ毎及びコンテンツの保持者毎にまとめる請求項１に記載の方法。

【請求項４】　前記認証サーバは、第１のユーザ端末に対してコンテンツ提供を許可する場合に、第１のユーザ端末が接続中である旨の情報を保持し、

前記コンテンツサーバは、第１のユーザ端末にコンテンツ提供を行う場合に、第１のユーザ端末が接続中である旨の情報を保持し、

第１のユーザ端末がコンテンツ提供を受けているときに、第２のユーザ端末から、第１のユーザ端末から送信されたユーザ識別情報と同一のユーザ識別情報を用いてコンテンツ要求がなされると、

認証サーバは、第１のユーザ端末の接続先のコンテンツサーバに該ユーザ識別情報に対応するユーザ端末が接続中であるか否かを問い合わせ、接続中であれば第２のユーザ端末からのコンテンツ要求を拒否し、接続中でなければ第２のユーザ端末へのコンテンツ提供可否の判定を継続する請求項１に記載の方法。

2

【請求項５】　インターネット上でディジタルコンテンツをユーザ端末に提供するコンテンツサーバであって、

ユーザ端末に提供するためのコンテンツを保持する手段と、

ユーザ端末からユーザ識別情報及びコンテンツ要求を受信すると、要求されたコンテンツをユーザ端末に提供できるか否かの判定を、該ユーザ端末をインターネットに接続するＩＳＰの認証サーバに要求する手段と、

認証サーバからコンテンツ提供可能の旨の通知を受けたときにユーザ端末にコンテンツを提供する手段とを有することを特徴とするコンテンツサーバ。

【請求項６】　インターネット上でディジタルコンテンツをユーザ端末に提供するために使用し、該ユーザ端末をインターネットに接続するＩＳＰにおける認証サーバであって、

コンテンツサーバから、ユーザ端末から要求されたコンテンツを該ユーザ端末に提供できるか否かの判定の要求を受信する手段と、

コンテンツサーバから受信したユーザ識別情報と該認証サーバが保有する登録データとを比較することによりユーザ認証を行い、コンテンツを該ユーザ端末に提供できるか否かの判定を行い、判定の結果をコンテンツサーバに送信する手段とを有することを特徴とする認証サーバ。

【請求項７】　前記コンテンツサーバが判定を要求する際に、該コンテンツサーバは前記ユーザ識別情報とともにコンテンツに関する情報を認証サーバに送信し、

該認証サーバは、該ユーザ識別情報に基づきユーザ認証を行うとともに、該コンテンツに関する情報に基づき前記ユーザ端末にコンテンツを提供できるか否かを判定し、

該コンテンツに関する情報の中の料金情報に基づき前記課金のための処理を行う請求項６に記載の認証サーバ。

【請求項８】　前記認証サーバは、第１のユーザ端末に対してコンテンツ提供を許可する場合に、第１のユーザ端末が接続中である旨の情報を保持し、

第１のユーザ端末がコンテンツ提供を受けているときに、第２のユーザ端末から、第１のユーザ端末から送信されたユーザ識別情報と同一のユーザ識別情報を用いてコンテンツ要求がなされると、

該認証サーバは、前記情報に基づきコンテンツ要求に係るユーザ識別情報の重複を認識し、第１のユーザ端末の接続先のコンテンツサーバに該ユーザ識別情報に対応するユーザ端末が接続中であるか否かを問い合わせ、接続中であれば第２のユーザ端末からのコンテンツ要求を拒否し、接続中でなければ第２のユーザ端末へのコンテンツ提供可否の判定を継続する請求項６に記載の認証サーバ。

【請求項９】　インターネット上でディジタルコンテンツをユーザ端末に提供するディジタルコンテンツ提供シ

ステムであって、
ユーザ端末に提供するためのコンテンツを保持するコンテンツサーバを地域毎に複数台有し、
各地域のコンテンツサーバは、各ＩＳＰのルータを介して各ＩＳＰに接続され、網終端装置を介して各地域のアクセス網に接続され、
各コンテンツサーバは、
ユーザ端末からユーザ識別情報及びコンテンツ要求を受信すると、要求されたコンテンツをユーザ端末に提供できるか否かの判定を、該ユーザ端末をインターネットに接続するＩＳＰの認証サーバに要求する手段と、
認証サーバからコンテンツ提供可能の旨の通知を受けたときにユーザ端末にコンテンツを提供する手段とを有し、
各ＩＳＰの認証サーバは、
コンテンツサーバから受信したユーザ識別情報と該認証サーバが保有する登録データとを比較することによりユーザ認証を行い、コンテンツを該ユーザ端末に提供できるか否かの判定を行い、判定の結果をコンテンツサーバに送信する手段とを有することを特徴とするシステム。

【請求項１０】　インターネット上でディジタルコンテンツをユーザ端末に提供する処理をコンピュータに実行させるプログラムであって、コンピュータに、
ユーザ端末に提供するためのコンテンツを取得及び保持する手順と、
ユーザ端末からユーザ識別情報及びコンテンツ要求を受信すると、要求されたコンテンツをユーザ端末に提供できるか否かの判定を、該ユーザ端末をインターネットに接続するＩＳＰの認証サーバに要求する手順と、
認証サーバからコンテンツ提供可能の旨の通知を受けたときにユーザ端末にコンテンツを提供する手順とを実行させるプログラム。

【請求項１１】　インターネット上でディジタルコンテンツをユーザ端末に提供するために使用し、該ユーザ端末をインターネットに接続するＩＳＰにおける認証サーバにおけるプログラムであって、認証サーバに、
コンテンツサーバから、ユーザ端末から要求されたコンテンツを該ユーザ端末に提供できるか否かの判定の要求を受信する手順と、
コンテンツサーバから受信したユーザ識別情報と該認証サーバが保有する登録データとを比較することによりユーザ認証を行い、コンテンツを該ユーザ端末に提供できるか否かの判定を行い、判定の結果をコンテンツサーバに送信する手順とを実行させるプログラム。

【請求項１２】　前記コンテンツサーバが判定を要求する際に、該コンテンツサーバは前記ユーザ識別情報とともにコンテンツに関する情報を認証サーバに送信し、
前記プログラムは、該ユーザ識別情報に基づきユーザ認証を行うとともに、該コンテンツに関する情報に基づき前記ユーザ端末にコンテンツを提供できるか否かを判定する手順と、
該コンテンツに関する情報の中の料金情報に基づき前記課金のための処理を行う手順とを認証サーバに実行させる請求項１１に記載のプログラム。

【請求項１３】　第１のユーザ端末に対してコンテンツ提供を許可する場合に、第１のユーザ端末が接続中である旨の情報を保持する手順と、
第１のユーザ端末がコンテンツ提供を受けているときに、第２のユーザ端末から、第１のユーザ端末から送信されたユーザ識別情報と同一のユーザ識別情報を用いてコンテンツ要求がなされると、
前記情報に基づきコンテンツ要求に係るユーザ識別情報の重複を認識し、第１のユーザ端末の接続先のコンテンツサーバに該ユーザ識別情報に対応するユーザ端末が接続中であるか否かを問い合わせ、接続中であれば第２のユーザ端末からのコンテンツ要求を拒否し、接続中でなければ第２のユーザ端末へのコンテンツ提供可否の判定を継続する手順とを認証サーバに実行させる請求項１１に記載のプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、インターネット上で有料ディジタルコンテンツをユーザに提供し、課金を行う技術に関する。

【０００２】

【従来の技術】近年、インターネット上で有料ディジタルコンテンツを提供するサービスが普及してきている。

【０００３】従来、コンテンツ保持者がディジタルコンテンツ視聴者に対してコンテンツを提供し料金回収を行うには、例えば、コンテンツ保持者又はコンテンツを預かったホスティング業者が、複数のＩＳＰユーザに対してコンテンツを提供し、独自の課金システムで課金を行ったり、１つのＩＳＰが複数のコンテンツ保持者からディジタルコンテンツを預かり、そのＩＳＰがユーザに課金していた。

【０００４】

【発明が解決しようとする課題】しかしながら、上記従来の技術によると、均質化された有料コンテンツの提供と課金を容易に実施することが出来なかった。

【０００５】本発明は上記の点に鑑みてなされたものであり、不特定多数が視聴可能な有料ディジタルコンテンツをユーザに提供し、効率的にユーザへの課金を行うことを可能とし、コンテンツ保持者はコンテンツを預けるだけでコンテンツ料金を回収することを可能とするディジタルコンテンツ提供方法及びサーバ並びにプログラムを提供することを目的とする。

【０００６】

【課題を解決するための手段】上記の目的を達成するために、本発明は次のように構成することができる。

【０００７】請求項１に記載の発明は、インターネット

上でディジタルコンテンツをユーザ端末に提供する方法であって、コンテンツサーバが、ユーザ端末に提供するためのコンテンツを保持し、ユーザ端末が、ユーザ識別情報及びコンテンツ要求をコンテンツサーバに送信し、コンテンツサーバが、要求されたコンテンツをユーザ端末に提供できるか否かの判定を、該ユーザ端末をインターネットに接続するＩＳＰの認証サーバに要求し、認証サーバが、前記ユーザ識別情報と該認証サーバが保有する登録データとを比較することによりユーザ認証を行い、コンテンツを該ユーザ端末に提供できるか否かの判定を行い、コンテンツサーバが、認証サーバからコンテンツ提供可能の旨の通知を受けたときにユーザ端末にコンテンツを提供し、前記ＩＳＰにおける課金手段が当該ユーザに当該コンテンツ提供に対する課金を行う。

【０００８】本発明によれば、ＩＳＰでユーザ認証を行い、コンテンツ視聴に対する課金を行うので、有料コンテンツの提供を効率的に行うことが可能となる。また、ユーザにとっては、新たにユーザ登録等を行う必要がないので、容易に有料コンテンツを視聴することが可能となる。

【０００９】請求項２に記載の発明は、請求項１の記載において、前記コンテンツサーバが前記ＩＳＰの認証サーバに判定を要求する際に、該コンテンツサーバは前記ユーザ識別情報とともにコンテンツに関する情報を認証サーバに送信し、認証サーバは、該ユーザ識別情報に基づきユーザ認証を行うとともに、該コンテンツに関する情報に基づき前記ユーザ端末にコンテンツを提供できるか否かを判定し、該コンテンツに関する情報の中の料金情報に基づき前記課金を行う。

【００１０】本発明によれば、コンテンツの内容に応じてアクセス制限を行うことが可能となる。

【００１１】請求項３に記載の発明は、請求項１の記載において、前記コンテンツサーバは、コンテンツ提供に関するログを蓄積し、クリアリングハウスサーバが、前記ログを収集し、該ログにおけるデータをＩＳＰ毎及びコンテンツの保持者毎にまとめる。

【００１２】本発明によれば、複数のＩＳＰ及び複数のコンテンツ保持者が混在したデータから、各ＩＳＰへの料金請求及び各コンテンツ保持者への料金支払いに必要なデータを生成することができる。これにより、コンテンツ保持者はコンテンツをコンテンツサーバに預けるだけでコンテンツ料金の回収を行うことが可能となる。

【００１３】請求項４に記載の発明は、請求項１の記載において、前記認証サーバは、第１のユーザ端末に対してコンテンツ提供を許可する場合に、第１のユーザ端末が接続中である旨の情報を保持し、前記コンテンツサーバは、第１のユーザ端末にコンテンツ提供を行う場合に、第１のユーザ端末が接続中である旨の情報を保持し、第１のユーザ端末がコンテンツ提供を受けているときに、第２のユーザ端末から、第１のユーザ端末から送

信されたユーザ識別情報と同一のユーザ識別情報を用いてコンテンツ要求がなされると、認証サーバは、第１のユーザ端末の接続先のコンテンツサーバに該ユーザ識別情報に対応するユーザ端末が接続中であるか否かを問い合わせ、接続中であれば第２のユーザ端末からのコンテンツ要求を拒否し、接続中でなければ第２のユーザ端末へのコンテンツ提供可否の判定を継続する。

【００１４】本発明によれば、１つのユーザＩＤを複数の端末で使用することによる不正アクセスを防止することが可能になる。また、コンテンツサーバと認証サーバの間でユーザログイン情報の状態不一致が生じた場合には、これを補正することが可能である。

【００１５】請求項５に記載の発明は、上記コンテンツサーバであり、請求項６～８に記載の発明は、上記認証サーバである。

【００１６】請求項９に記載の発明は、インターネット上でディジタルコンテンツをユーザ端末に提供するディジタルコンテンツ提供システムであって、ユーザ端末に提供するためのコンテンツを保持するコンテンツサーバを地域毎に複数台有し、各地域のコンテンツサーバは、各ＩＳＰのルータを介して各ＩＳＰに接続され、網終端装置を介して各地域のアクセス網に接続され、各コンテンツサーバは、ユーザ端末からユーザ識別情報及びコンテンツ要求を受信すると、要求されたコンテンツをユーザ端末に提供できるか否かの判定を、該ユーザ端末をインターネットに接続するＩＳＰの認証サーバに要求する手段と、認証サーバからコンテンツ提供可能の旨の通知を受けたときにユーザ端末にコンテンツを提供する手段とを有し、各ＩＳＰの認証サーバは、コンテンツサーバから受信したユーザ識別情報と該認証サーバが保有する登録データとを比較することによりユーザ認証を行い、コンテンツを該ユーザ端末に提供できるか否かの判定を行い、判定の結果をコンテンツサーバに送信する手段とを有する。

【００１７】本発明によれば、どのＩＳＰを使用してもコンテンツ品質に差がでないようにコンテンツを提供することが可能となる。

【００１８】請求項１０～１３に記載の発明は、上記各サーバにおけるプログラムである。

【００１９】

【発明の実施の形態】本発明のディジタルコンテンツ提供システムの原理構成を図１に示す。まず、図１を用いて本発明のディジタルコンテンツ提供システムの概要について説明する。

【００２０】図１に示すように、本発明のディジタルコンテンツ提供システムは、ＩＳＰユーザのユーザ端末１、コンテンツサーバ２、当該ＩＳＰのＩＳＰ認証サーバ３、クリアリングハウスサーバ４を有し、各々がインターネット５に接続された構成をとる。なお、同図におけるＩＳＰは当該ユーザがインターネット接続プロバイ

ダとして加入しているＩＳＰである。

【００２１】同図に示すコンテンツ保持者サーバ６は、コンテンツ保持者が有するサーバであり、コンテンツ保持者はディジタルコンテンツの著作権を保持する者もしくは著作権運用を委託された者であり、ディジタルコンテンツを広く不特定多数の潜在客に見てもらいたいと考え、コンテンツサーバ２に自己のディジタルコンテンツを預ける。

【００２２】ＩＳＰはインターネットサービスプロバイダである。本発明では、当該ＩＳＰのユーザがコンテンツサーバ２のコンテンツを取得、視聴した場合、このＩＳＰが当該ユーザにコンテンツ料金を課金する。課金自体はＩＳＰにおける課金サーバ等にて従来の方法を用いて行うことができる。

【００２３】ユーザ端末１は、コンテンツの視聴を希望するユーザの端末であり、コンテンツサーバ２に対し、コネクションを開設し、サーバ内のディジタルコンテンツを利用する。

【００２４】コンテンツサーバ２は、例えば、コンテンツホスティング業者が保有するサーバであり、コンテンツ保持者のディジタルコンテンツのコピーを保持する。なお、コンテンツサーバ２をＩＳＰが保有する場合もある。

【００２５】クリアリングハウスサーバ４は、例えば、クリアリングハウス業者が保有するサーバであり、ＩＳＰが徴収したコンテンツ料金を、コンテンツ保持者、コンテンツホスティング事業者に再配分するための処理を行う。なお、クリアリングハウスサーバ４とコンテンツサーバ２を１つのサーバで構成することも可能である。

【００２６】ＩＳＰ認証サーバ３は、ＩＳＰの加入ユーザの情報を保持し、ユーザ認証を行うことによりユーザのコンテンツに対するアクセスの許否を判断する。なお、ＩＳＰ認証サーバ３については、当該ＩＳＰがユーザ認証等に使用する既存のサーバを使用することができる。

【００２７】なお、各サーバはＣＰＵ、ハードディスク、入出力装置、通信制御装置等を有するコンピュータに、本発明における処理を実行するプログラムを搭載することにより実現できる。

【００２８】図１のディジタルコンテンツ提供システムの動作概要について次に説明する。

【００２９】ステップ１）まず、コンテンツ保持者はコンテンツサーバ２に対して、ディジタルコンテンツのコピーを預けておく。また、あわせて当該コンテンツの料金情報もコンテンツサーバ２に通知しておく。料金情報とは、例えば、そのコンテンツは１回の視聴で１００円、もしくは月額５００円コースであれば視聴可能等の情報である。

【００３０】ステップ２）ユーザは、ユーザ端末１からインターネット５を経由して、有料コンテンツの視聴要求をコンテンツサーバ２に対して行う。そのとき、コンテンツサーバ２はユーザにアクセスＩＤやパスワードの入力を要求し、ユーザはそれらを入力する。なお、そのアクセスＩＤやパスワードは、当該ユーザが加入しているＩＳＰにてインターネット接続時に使用するものと同一である。

【００３１】ステップ３）次に、コンテンツサーバ２は、ＩＳＰ認証サーバ３に対して、当該ユーザにコンテンツの視聴を許可するかどうかの問い合わせを行う。ここでの問い合わせ情報には、（どのユーザが、どのコンテンツを、どのような課金で）という情報を含む。

【００３２】上記問い合わせ情報における“どのユーザが”とは、ユーザが入力したアクセスＩＤとパスワードであり、これをもってＩＳＰ認証サーバは、当該ＩＳＰの顧客であるかどうか認証する。“どのコンテンツを”とは、ユーザが視聴を要求したコンテンツを識別するための情報のことであり、ファイル名や、コンテンツ保持者名、ライブ番組名等を含む。“どのような課金で”とは、ステップ１でコンテンツ保持者サーバ６がコンテンツサーバ２にコンテンツを預けたときに指定した料金情報である。

【００３３】ステップ４）問い合わせ情報を受信したＩＳＰ認証サーバ３は、問い合わせ内容を検証することにより、ユーザにコンテンツを見せてよいかどうか判断し、判断の結果をコンテンツサーバ２に返す。

【００３４】判断の基準は種々設定することが可能であるが、課金を実行するためには当該ユーザが当該ＩＳＰのユーザであることが必要であるので、ＩＤとパスワードとから当該ユーザが自社顧客であるか否かを少なくとも判断する。その他の判断としては、例えば、該当コンテンツが競合他社のものであった場合に視聴拒否したり、コンテンツの内容が当該ユーザにとって適切でない場合や、ユーザがＩＳＰに対して料金滞納している場合等に視聴拒否する判断を行うことが可能である。ＩＳＰ認証サーバがコンテンツ提供可否を判断するために、コンテンツサーバからＩＳＰに対して予めコンテンツの内容を記載した番組表のような情報を送信しておくこともできる。例えば、その番組表にないコンテンツ要求を拒否する等の制御が可能になる。

【００３５】ここで、ＩＳＰ認証サーバ３が視聴許可をコンテンツサーバ２に対して返す場合には、ＩＳＰは問い合わせ内容に含まれていた課金情報により当該ユーザに課金を行い、視聴拒否させるならコンテンツの課金は行わない。

【００３６】ステップ５）コンテンツサーバ２はＩＳＰ認証サーバ３から視聴許可がおりれば、コンテンツをユーザ端末１に配信する。視聴が拒否された場合には、ユーザ端末１からのコンテンツへのアクセスを許否する。また、コンテンツサーバ２は、認証の結果を認証ログとして保持する。

【００３７】続いて、クリアリングハウスサーバ４が料金回収のための処理を行うこととなる。料金回収の方法を、図２に示す概念図を用いて説明する。

【００３８】ステップ１１）ＩＳＰは、視聴許可したコンテンツについて、指定の料金情報に従って課金サーバ等を用いてユーザに課金し、ユーザから料金を徴収する。コンテンツに対する課金は、通常のインターネット接続に対する課金に含めて行うことが可能である。

【００３９】ステップ１２）クリアリングハウスサーバ４は、コンテンツサーバ２から認証ログを収集する。これにより、各ＩＳＰがどのユーザに何をいつどの料金で視聴許可したのか等の情報がクリアリングハウスサーバ４に集積される。

【００４０】ステップ１３）そして、クリアリングハウス業者は、クリアリングハウスサーバ４に集積されたログに従って、代行徴収手数料を差し引いた視聴料金をＩＳＰに対して請求する。

【００４１】ステップ１４）ＩＳＰは自社のログからステップ１３の請求が妥当であると判断すれば、請求金額をクリアリングハウス業者に対し支払う。

【００４２】ステップ１５）必要に応じて、クリアリングハウス業者はコンテンツホスティング業者に対し、設備使用料を支払う。

【００４３】ステップ１６）クリアリングハウス業者は、コンテンツ保持者に対し、該当コンテンツの視聴料を支払う。

【００４４】ステップ１７）クリアリングハウス業者は、あわせて、視聴のログをコンテンツ保持者に対して提出する。

【００４５】次に、上記ディジタルコンテンツ提供システムをより詳細に説明する。

【００４６】（システム構成）図３、４に本発明のディジタルコンテンツ提供システムの構成の具体例を示す。この例はコンテンツサーバを地域分散設置とする場合の例であり、図３に全体構成を示し、図４に各拠点の構成を示す。

【００４７】図３に示すように、各地にコンテンツサーバを分散させることにより、ユーザに提供するコンテンツの品質を均質化することができる。また、図４に示すように、コンテンツサーバを拠点ビル内で各ＩＳＰ社と直接接続することにより、各ＩＳＰのネットワーク構成に依存せずにコンテンツを提供することが可能となり、更に品質を均質化することができる。

【００４８】従って、ユーザがどのＩＳＰを使ってもほとんど同じ品質となるので、コンテンツ保持者がコンテンツの価格を決定することができる。

【００４９】次に、上記ディジタルコンテンツ提供システムにおける主要な技術として認証技術と不正アクセス許否技術について説明する。

【００５０】（認証技術）図５に、コンテンツサーバ２が有するテーブル類を示す。また、図６に、ＩＳＰ認証サーバ３が有するテーブルを示す。図５、図６を用いてコンテンツサーバ及びＩＳＰ認証サーバにおける動作をより詳細に説明する。

【００５１】図５において、コンテンツレポジトリ７とはコンテンツ格納部であり、ユーザに提供するためのコンテンツを格納する。コンテンツ管理表８は、コンテンツ毎の課金パターン、アクセス制限、所有者等の項目を有する。ＩＳＰ認証サーバ管理表９は、接続要求したユーザＩＤのドメイン名からどのＩＳＰ認証サーバに認証要求を発行すべきかを決定するための情報として、ドメイン名及びそのドメイン名に対応するＩＳＰ認証サーバドレスを格納する。また、現在接続中のユーザの一覧を示す接続ユーザ表１０、及び認証要求、切断通知毎にイベント情報を記録する認証ログ１１を有する。

【００５２】また、図６に示すように、ＩＳＰ認証サーバ３が保持するユーザ管理表は、ユーザＩＤ，パスワード、アクセス制限、状態を有する。

【００５３】ユーザ認証における動作は次の通りである。

【００５４】まず、ＩＳＰ１に加入しているユーザが、ユーザＩＤ及びパスワードを入力することによってコンテンツＡへのアクセス要求を送信する（ステップ２１）。続いて、コンテンツサーバ２において、コンテンツ管理表８が参照され、コンテンツＡの課金パターン、アクセス制限情報、及びコンテンツの所有者名を抽出する（ステップ２２）。

【００５５】そして、コンテンツサーバ２はユーザが加入するＩＳＰ１のドメイン名ｉｓｐ１からＩＳＰ１認証サーバのアドレスをＩＳＰ認証サーバ管理表９から検索し、そのアドレス宛にユーザＩＤとパスワードとともにコンテンツに関する情報（コンテンツ名、所有者、料金情報等）を送信することにより認証を要求する（ステップ２３）。このとき、その認証要求の内容が認証ログ１１に記録される。

【００５６】認証要求を受けたＩＳＰ１認証サーバでは、図６に示すユーザ管理表を参照し、当該ユーザが自社の顧客であるか否か、アクセス制限に該当するか否か等を認証する。また、ＩＳＰ１認証サーバは視聴可能コンテンツ情報又は視聴禁止コンテンツ情報を有し、この情報と要求されたコンテンツ情報とを比較することにより、コンテンツを提供するか否かを判断する。また、コンテンツサーバから送信された当該コンテンツの料金に関する情報を当該ユーザに対するコンテンツ視聴料金課金のために使用する。

【００５７】そして、その認証結果をコンテンツサーバ２に返送する。

【００５８】なお、ＩＳＰ１認証サーバがコンテンツアクセスを許容した場合には、図６に示すテーブルの“状態”の項目が“接続中”となる。また、当該ユーザ端末

がコンテンツサーバ２に接続し、コンテンツの提供を受ける場合には、当該ユーザのＩＤ等が現在接続中のユーザとして接続ユーザ表１０に記載される。また、コンテンツ提供終了時には接続ユーザ表１０から当該ユーザが削除され、コンテンツサーバはコンテンツ提供サービスを完了した旨をＩＳＰ１認証サーバに通知し、ＩＳＰ１認証サーバは当該ユーザに対応するユーザ管理表の“状態”を”未接続“とする。これらは、後述する不正アクセス許否において用いられる。

【００５９】（不正アクセス許否技術）コンテンツサーバ２へのアクセス認証を上述のようにユーザＩＤとパスワードで行う場合、他人のアクセスＩＤとパスワードを不正に利用し、1つのＩＤで同時に複数のユーザがコンテンツを取得するという不正アクセスが行われる危険がある。このような不正アクセスを防止するために、図５及び図６において説明した接続ユーザ表及びユーザ管理表を用いる。以下、不正アクセス防止のための処理を図７及び図８を用いて説明する。

【００６０】図７において、まず、ユーザが札幌に設置されたディジタルコンテンツサーバに対してアクセス要求を行い、アクセスが許可されて該当コンテンツを視聴しているものとする（ステップ３１～３３）。このとき、ＩＳＰ認証サーバは、ユーザ管理表における当該ユーザＩＤに対応する状態を“接続中@札幌”とする。これは、当該ユーザに札幌のコンテンツサーバがサービス供与中であるということを意味する。また、札幌のコンテンツサーバにおける接続ユーザ表に当該ユーザＩＤ（ｉｄ１@ｉｓｐ１）を追加する。

【００６１】このユーザが接続中に、他のユーザが、例えば東京のコンテンツサーバに対して同じユーザＩＤとパスワードでコンテンツアクセス要求を行った場合（ステップ３４）、認証要求を受けたＩＳＰ認証サーバは、上記ユーザ管理表により、そのユーザＩＤに対応するユーザは接続中であること認識する（ステップ３４、３５）。

【００６２】このように、ＩＳＰ認証サーバが、接続中のユーザＩＤに対して再び認証要求を受けた場合（２重アクセス検出）、ＩＳＰ認証サーバは札幌のコンテンツサーバに対して、最初のユーザがサービス供与中であるかどうか（接続ユーザ表に当該ユーザＩＤがあるかどうか）を問い合わせ、最初のユーザが接続中であることが判明すれば、ＩＳＰ認証サーバは認証要求に対して接続拒否を返す（ステップ３６～３８）。

【００６３】一方、札幌のコンテンツサーバにおいて、当該ユーザが接続中でないことが確認された場合には、東京のコンテンツサーバの認証要求（ステップ３５）に対して認証作業を継続し、認証が成功し、コンテンツ視聴可能であると判断した場合には、東京のコンテンツサーバから当該ユーザに対してコンテンツを提供する。

【００６４】図８は、ＩＳＰ認証サーバにおける処理を示すフローチャートである。

【００６５】あるアクセスポイントにユーザからのアクセスがあると（ステップ４１）、ユーザ認証を行い（ステップ４２）、認証がＯＫであれば、ユーザ管理表を参照して当該ユーザが接続中（ログイン中）か否かを判定し、認証がＮＧであれば接続を拒否する。次に、当該ユーザが接続中（ログイン中）であるか否かをユーザ管理表を参照して確認し（ステップ４３）、未接続であれば接続を許可する。接続中（ログイン中）の場合には、当該接続中のコンテンツサーバに状態を問い合わせ（ステップ４４）、コンテンツサーバから接続中の回答があった場合には接続を拒否し、未接続のときには接続を許可する（ステップ４５）。

【００６６】なお、上記のように最初のユーザアクセスに係るコンテンツサーバに接続中か否かを確認することにより、コンテンツサーバのリブート、認証パケットのネットワーク上での紛失等により、最初のユーザに関するコンテンツサーバでのサービス供与が終了しているにもかかわらず、ＩＳＰ認証サーバだけがサービス提供中であると認識している状態不一致が生ずる場合でも的確に接続許否の判断を行うことが可能となる。

【００６７】また、ＩＳＰ認証サーバで２重アクセス検査を行うことにより、異なるコンテンツサーバに属するユーザから不正アクセスが試みられた場合でも２重アクセスを検知することができる。

【００６８】（課金処理）次に、図２で説明した料金回収のためにクリアリングハウスサーバ４が行う処理を図９を用いて説明する。

【００６９】クリアリングハウスサーバ４は、図９の（ａ）に示す認証ログを各コンテンツサーバから収集する。収集した認証ログは、視聴日時、ユーザに課金を行うＩＳＰ、ユーザ、コンテンツ保持者名、コンテンツ名、金額等の情報を有する。

【００７０】このように複数のＩＳＰと複数の保持者が混在したログ情報に対し、ＩＳＰ毎に名寄せし、図９（ｂ）に示す形にすることにより、視聴料金を各ＩＳＰに請求することが可能となる。また、保持者名毎に名寄せし、図９（ｃ）に示す形にすることにより、コンテンツ保持者に対しコンテンツの視聴料を支払うことが可能となる。更に、コンテンツ保持者に視聴ログを提供することにより、コンテンツ保持者はどのユーザが、いつ、どのコンテンツを視聴したかを把握することが可能となる。

【００７１】本発明は、上記の実施例に限定されることなく、特許請求の範囲内で種々変更・応用が可能である。

【００７２】

【発明の効果】上記のように、本発明によれば、コンテンツ保持者はコンテンツホスティング業者に対し、コンテンツを預けることで独自の課金システムを使用するこ

となくコンテンツ料金を得ることができるようになる。

【００７３】また、コンテンツサーバをエンドユーザに近いところに複数配置することにより、どのＩＳＰのエンドユーザもほぼ同質なコンテンツ品質を得ることができるので、コンテンツ保持者はＩＳＰを選ぶことなく、均一な料金設定を行うことが可能となる。

【００７４】また、本発明におけるクリアリングハウスサーバの処理により、各ＩＳＰに対し、当該ＩＳＰに関わる情報だけを選択してそのＩＳＰに視聴料金を徴収することが可能となる。一方、各コンテンツ保持者に対しては、当該コンテンツ保持者のコンテンツに関わる情報だけ選択して、視聴料を支払うことが可能となる。

【００７５】更に、本発明においてはＩＳＰにおける既存の認証、課金システム及び登録データを用いて認証、課金を行うことができるため、新たな顧客データベースを作成することなく、上記のような効果的な料金徴収を実現することが可能となる。

【００７６】従って、本発明によれば、ＩＳＰ－Ａのユーザがｉｓｐ－Ｂのコンテンツを見たときに、ＩＳＰ－Ａからコンテンツ料金の課金がユーザに対してなされ、一方、その逆として、ＩＳＰ－Ｂのユーザがｉｓｐ－Ａのコンテンツを視聴した場合、ＩＳＰ－Ｂからコンテンツ料金の課金がユーザに対してなされる。このように、従来と異なり、コンテンツ保持者とＩＳＰとのＮ：Ｍの関係を構築することが可能となる。

【図面の簡単な説明】

【図１】本発明のディジタルコンテンツ提供システムの原理構成を示す図である。

【図２】料金回収の方法を説明するための図である。

【図３】ディジタルコンテンツ提供システムの構成を示す図である。

【図４】ディジタルコンテンツ提供システムの構成を示す図である。

【図５】コンテンツサーバが有するテーブル類を示す図である。

【図６】ＩＳＰ認証サーバが有するテーブル類を示す図である。

【図７】不正アクセス防止技術を説明するための図である。

【図８】ＩＳＰ認証サーバにおける処理を示すフローチャートである。

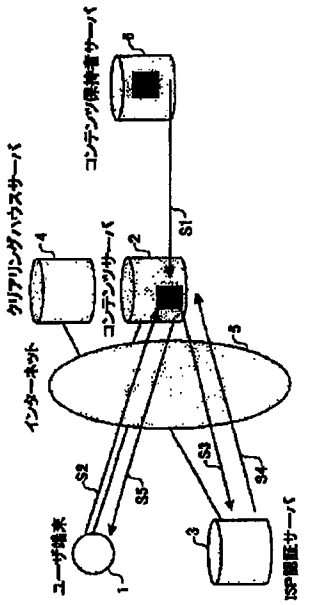
【図９】クリアリングハウスサーバにおける処理を説明するための図である。

【符号の説明】

１　ユーザ端末
２　コンテンツサーバ
３　ＩＳＰ認証サーバ
４　クリアリングハウスサーバ
５　インターネット
６　コンテンツ保持者サーバ
７　コンテンツレポジトリ
８　コンテンツ管理表
９　ＩＳＰ認証サーバ管理表
１０　接続ユーザ表
１１　認証ログ

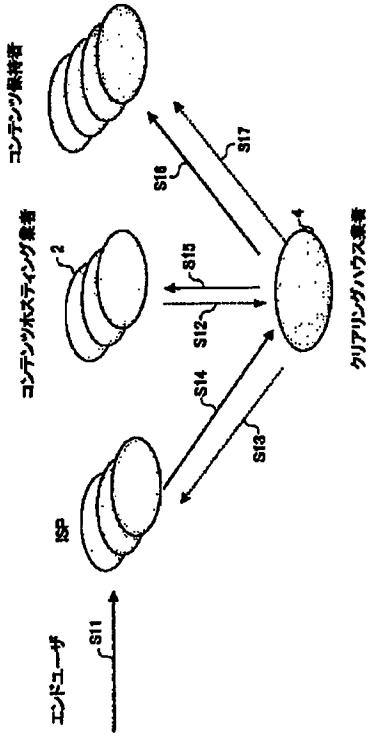
【図１】

本発明のディジタルコンテンツ提供システムの原理構成を示す図



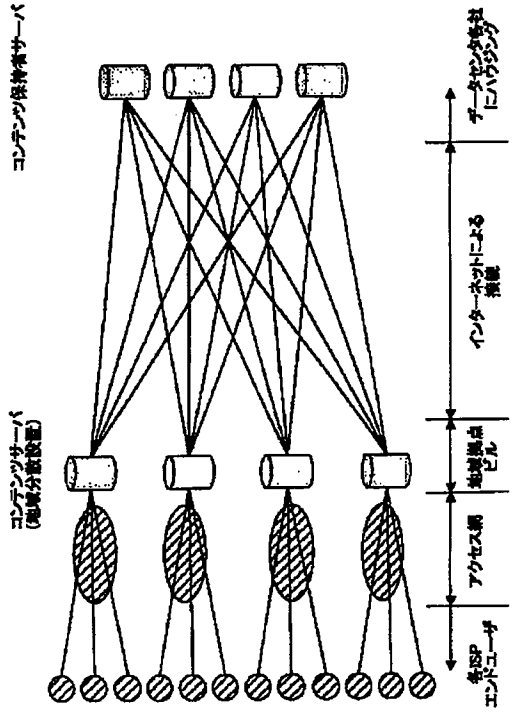
【図２】

料金回収の方法を説明するための図



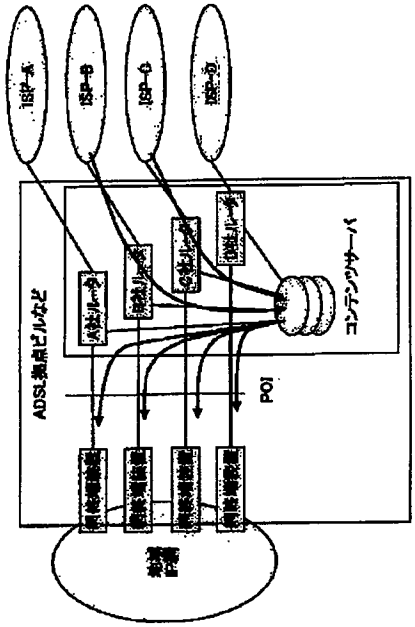
【図３】

ディジタルコンテンツ提供システムの構成を示す図



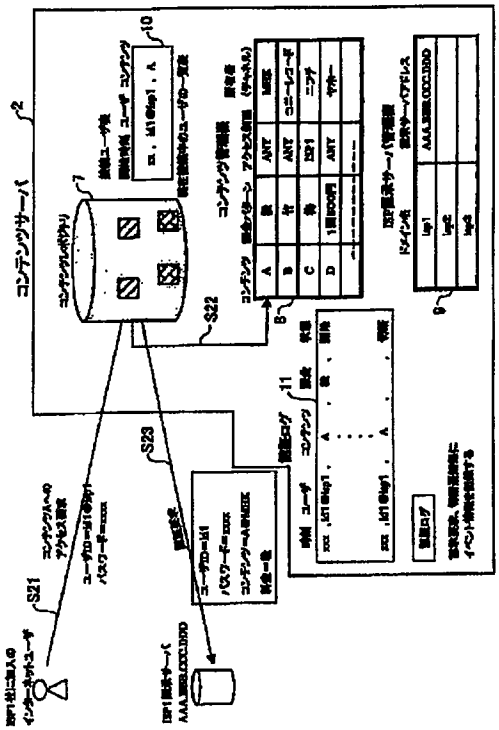
【図４】

ディジタルコンテンツ提供システムの構成を示す図



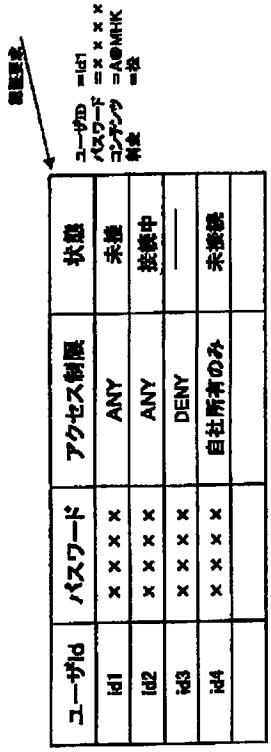
【図５】

コンテンツサーバが有するテーブル類を示す図



【図６】

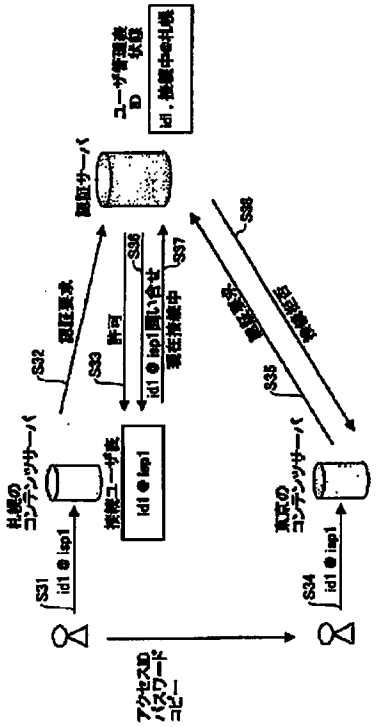
ISP認証サーバが有するテーブル類を示す図



ユーザId	パスワード	アクセス制限	状態
id1	××××	ANY	未接
id2	××××	ANY	接続中
id3	××××	DENY	——
id4	××××	自社所有のみ	未接続

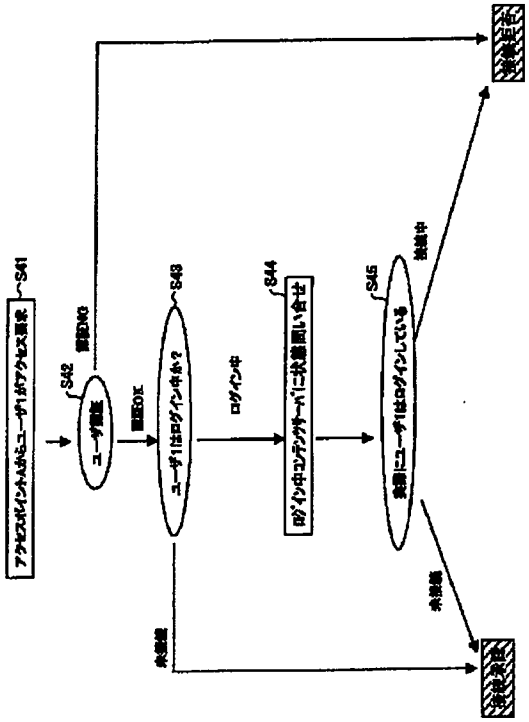
【図７】

不正アクセス防止技術を説明するための図



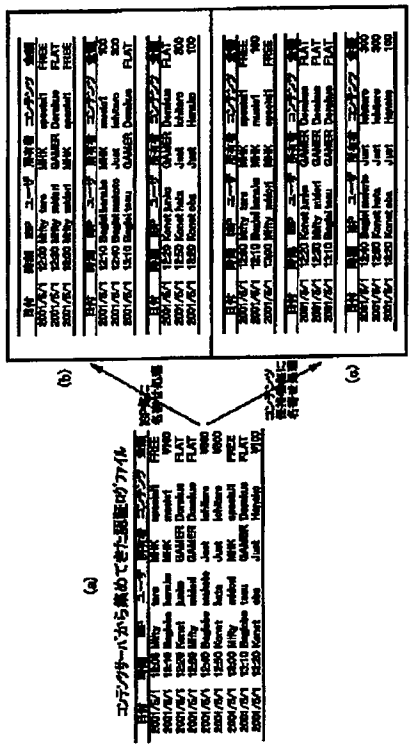
【図８】

IPS認証サーバにおける処理を示すフローチャート



【図９】

クリアリングハウスサーバにおける処理を説明するための図



フロントページの続き

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)
Ｇ０６Ｆ	17/60	ＺＥＣ	Ｇ０６Ｆ	17/60	ＺＥＣ
	12/00	５３７		12/00	５３７Ｄ
		５４５			５４５Ｍ
	12/14	３２０		12/14	３２０Ｃ